B12

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31839 A2

(51) International Patent Classification[7]: H04L 9/08, G06F 1/00

(21) International Application Number: PCT/US00/29184

(22) International Filing Date: 21 October 2000 (21.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/425,861 23 October 1999 (23.10.1999) US

(71) Applicant: LOCKSTREAM CORP. [US/US]; 13033 Bellevue-Redmond Road, Bellevue, WA 98005 (US).

(72) Inventor: SEARLE, Scott; 218 Main Street, Suite 441, Kirkland, WA 98033 (US).

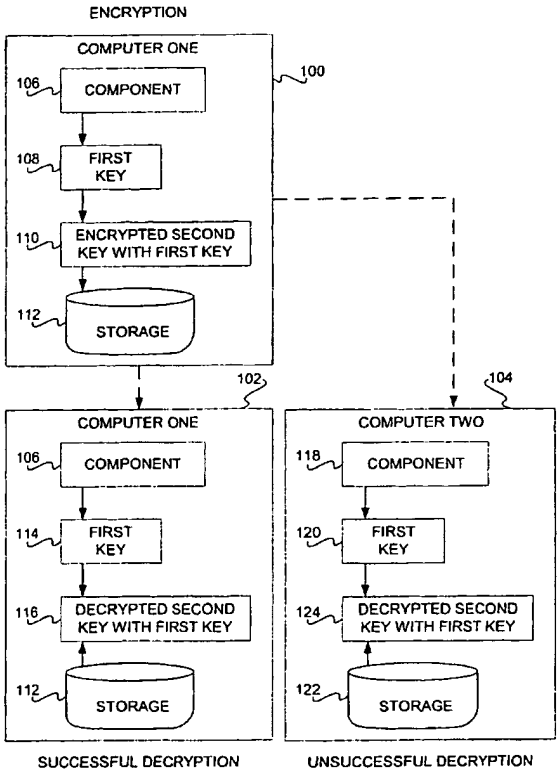
(74) Agents: LERNER, Lawrence, I. et al.; Lerner, David, Littenberg,, Krumholz & Mentlik, LLP, 600 South Avenue West, Westfield, NJ 07090 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: KEY ENCRYPTION USING CLIENT-UNIQUE ADDITIONAL KEY



[Continued on next page]

WO 01/31839 A2

Published:
-- *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(57) Abstract: Encryption of a key using another key that is unique and particular to a given client is disclose. In one embodiment, a computer-implemented method determines a first key that is unique and particular to the client, without user intervention. In varying embodiments, this key can be one or more of: a processor identifier, a network card address, an IP address, a checksum of a component, a serial number of a hard disk drive, a number of cylinders of a hard disk drive, and a user name in a registry file. At least a second key that provides access to information, such as multimedia information, is encrypted with this first key. The second key as encrypted with the first key may be stored on a storage.

KEY ENCRYPTION USING CLIENT-UNIQUE ADDITIONAL KEY

TECHNICAL FIELD

This invention relates generally to encryption and decryption of information, such as multimedia information, accomplished via a key, and more particularly to additional encryption and decryption of the key using a client-unique additional key for fraud prevention.

BACKGROUND ART

The Internet has become a popular manner by which to purchase multimedia information such as music, a phenomenon that seemingly will only increase over time as more consumers have the ability to connect to the Internet, and as their connections are at greater bandwidths to permit other multimedia information, such as video, to also be easily purchased. While actors, artists and companies responsible for producing and distributing such multimedia information generally applaud new manners of distribution, they are nevertheless somewhat concerned about the Internet and other manners by which digital versions of their content can be distributed. This is because a copy of a digital version of content can easily be duplicated illegally by consumers, potentially decreasing the revenue taken in by the rightful owners of the content.

One solution that has been suggested and used within the prior art is the encryption of multimedia information via known encryption schemes. Usually, and especially in the context of multimedia information purchased by end consumers, the information is encrypted with a key. Knowledge of the key, therefore, is required to decrypt the information; without the key, the encrypted information is unintelligible. Thus, even if many digital copies of a particular song or movie were distributed over the Internet to end users all over the world, unless a given end user knows the key to unlock the encrypted copy, the song or movie is useless.

A barrier to the overall effectiveness of this approach is, however, that little deters a consumer who has purchased encrypted multimedia information from sharing the key provided to him or her with others, or even from posting the key on the Internet along with the encrypted information. While content owners can assign each purchaser of content a unique key, such that illegal distribution of the key can be traced back to the original purchaser, this puts the onus of enforcement on the owners themselves, which will likely

be time-consuming and expensive. Furthermore, the owners are put in the uncomfortable position of bringing action against their own customers, which may lead to public relations and other problems where it turns out that the key assigned to a particular consumer was distributed on a large scale through no fault of the consumer – for example, where the key was stolen from the consumer.

A solution to this and other problems is described in the copending, cofiled, and coassigned application entitled "Encryption Using a User-Known and Personally Valuable Key to Deter Key Sharing," attorney docket 1019.001US1. In this application, the key used for encryption of the information is known to the user and personally valuable to him or her, such as a social security number, driver's license number, credit card number, etc. A user is thus motivated not to share the key with others, since the key itself has personal value to him or her.

However, this solution does not prevent the user from using or copying the information, such as text or multimedia information, on multiple computers or devices owned or accessible by him or her. For example, a user may have a desktop computer, a portable electronic device, and a laptop computer, all of which the user can copy the information to, for use on any such device. However, this may be against the licensing terms to which the user agreed when first purchasing or otherwise obtaining the information. The seller or provider of the information has little recourse in this situation within the prior art.

For these and other reasons, then, there is a need for the present invention.

DISCLOSURE OF INVENTION

The invention provides for encryption of a key using another key that is unique and particular to a given client, such as a desktop computer, a laptop computer, a portable electronic device, etc., for fraud prevention and other purposes. In one embodiment, a computer-implemented method determines a first key that is unique and particular to the client, without user intervention. In varying embodiments of the invention, this key can be one or more of: a processor identifier, a network card address, and a user name in a registry file. The key may also be one or more of: serial numbers and/or the number of cylinders of attached hard disk drives, checksums of the read-only memory (ROM) or other system components, the Internet Protocol (IP) address of the computer or system, and a combination of installed cards, such as sound, video, SCSI, and other cards, as the

key. At least a second key that actually provides access to information, such as multimedia information, is then encrypted with this first key. (Other information may also be encrypted with the first key.) The second key as encrypted with the first key may be stored on a storage, such as a non-volatile memory or a hard disk drive.

Embodiments of the invention provides for advantages not found within the prior art. When decryption of the information is desired, in one embodiment, the second key first must be decrypted using the first key. The first key is thus redetermined and used to decrypt the second key. Because the first key is specific to the underlying computer or device, if the encrypted second key is moved to another computer or device, it will not be decrypted successfully. Thus, users are restrained from copying the information to other clients other than that on which they first stored the information, without, for example, reregistering the information with the seller or other provider.

Other embodiments of the invention enhance fraud prevention and security in still other ways. For example, the recording inputs may be varied when multimedia information is played back, so that any illicit recording will result in an undesirable copy of the information. As a further example, various checksums can be determined to ensure that the user has not made illicit changes to the playback software or other playback mechanism, as well as various system checks to detect known piracy programs that may be running on the system. In addition, a server can be contacted, for example, over the Internet, to update the player software or other playback mechanism, as well as the system checks that are to be performed.

The invention includes computer-implemented methods, machine-readable media, computerized systems, and computers of varying scopes. Other aspects, embodiments and advantages of the invention, beyond those described here, will become apparent by reading the detailed description and with reference to the drawings.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a diagram illustrating the operation of an embodiment of the invention;

FIG. 2 is a flowchart of a method according to an embodiment of the invention;

FIG. 3 is a block diagram of a representative computer or computerized device in conjunction with which embodiments of the invention may be practiced;

FIG. 4 is a flowchart of a checksum verification method according to an embodiment of the invention;

FIG. 5 is a flowchart of a piracy-signature detection method according to an embodiment of the invention; and,

FIG. 6 is a diagram illustrating the manner by which recording inputs can be dynamically varied during multimedia information playback to thwart piracy in accordance with an embodiment of the invention.

MODE(S) FOR CARRYING OUT INVENTION

In the following detailed description of exemplary embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific exemplary embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical and other changes may be made without departing from the spirit or scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

Some portions of the detailed descriptions which follow are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as processing or computing or calculating or determining or displaying or the like, refer to the action and processes of a computer system, or similar

electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Cryptography Background

In this section of the detailed description, a brief summary of cryptography is presented. Embodiments of the invention are not limited to a particular scheme by which to perform encryption and decryption. Those of ordinary skill within the art can appreciate that many such different schemes exist, and can be used in accordance with embodiments of the invention. One common scheme that can be used by embodiments of the invention, but to which the invention itself is not limited, is known as the Data Encryption Standard, or DES. Other known schemes include, Rivest Cipher #4 (RC4), Rivest Cipher #2 (RC2), SKIPJACK, International Data Encryption Algorithm (IDEA), Blowfish, Twofish, triple DES (3DES), EEE3, EDE3, EEE2, and EDE2.

Cryptography generally is the conversion of data into a secret code, so that, for example, it can be transmitted over a public network, such as the Internet. The original data is converted (encrypted) into a coded equivalent via an encryption algorithm, or scheme. The encrypted data is decoded (decrypted) at the receiving end and turned back into the original data. The encrypted data is typically unintelligible.

An encryption scheme uses a key, for example, a binary number that is between 40 to 128 bits in length. The data is "locked" for sending by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code, restoring it to its original binary form. The particular types of keys that are used by embodiments of the invention are described in a later section of the detailed description. A key used by an encryption or decryption scheme is generally referred to as a code that is combined in some manner with the original data or information to encrypt the data or information for security purposes.

It is noted that in conjunction with embodiments of the invention, a key can be a number, characters, or any combination thereof. That is, where a key is referred to herein as a number, this is one example of what a key can be. Those of ordinary skill within the art can appreciate that the invention is not so limited, and that keys made up of characters,

as well as numbers and characters, in addition to just numbers, are also applicable to embodiments of the invention.

Operation of an Embodiment of the Invention

In this section of the detailed description, the operation of one particular embodiment of the invention is described. The invention itself, however, is not limited to the description of this section. The description of this section is made in conjunction with FIG. 1.

FIG. 1 is a diagram showing an encryption 100 situation, a successful decryption 102 situation, and an unsuccessful decryption 104 situation, according to an embodiment of the invention. In the encryption 100, a component 106 of computer one is used to determine a first key 108. The first key 108 is unique and particular to computer one. The component 106 has an identifier such that it can be used to particularly and uniquely identify computer one. That is, the identifier of the component 106 is used as the first key 108, such that the first key 108 is unique and particular to computer one.

The invention is not particularly limited to a given type of component 106. In one embodiment, the component 106 is one or more of the following: a processor that has a unique serial number or other identifier, such as an Intel Pentium III processor having such an identifier; a network card having a unique media access controller (MAC) address; and, in embodiments of the invention utilizing a version of the Microsoft Windows operating system, the user name as saved in a registry file of the operating system. The component may also be one or more of: a hard disk drive having serial numbers and/or a particular number of cylinders, read-only memory (ROM) or other system components (for the providing of checksums thereof), the Internet Protocol (IP) address of the computer or system, and a combination of installed cards, such as sound, video, SCSI, and other cards.

At least a second key that has been used to encrypt information, such as multimedia information, is then encrypted with the first key in 110. For example, the second key may be user-known and personally valuable information, as described in the copending, coassigned, and cofiled patent application entitled "Encryption Using a User-Known and Personally Valuable Key to Deter Key Sharing," attorney docket 1019.001US1. In that case, information, such as text information or multimedia information such as video, audio, music, and image information, is encrypted using a key that is user known and personally valuable, such as a credit card number or a driver's

license number. Thus, in 110, this key is encrypted using the first key 108, which is unique and particular to computer one as based on an identifier of the component 106 that uniquely and particularly identifies computer one. The encrypted second key is stored on the storage 112, which can be a non-volatile memory such as a flash memory, or a hard disk drive, etc.. The invention is not limited to a particular type of storage 112.

In one embodiment of the invention, more information than just the second key is encrypted using the first key. For example, user identification, server addresses, playback information, program configuration, etc., may be configured, in addition to the second key.

The statement that the second key is encrypted using a first key uniquely and particularly identifying computer one (which can be referred to as the client computer) is now described. Those of ordinary skill within the art understand that encryption is typically performed by a key that is any number of bits in length, such as between 40 and 128 bits in length. Each bit is either a 1 or a 0. The statement that information is encrypted using a key as described in the previous paragraphs means that the ultimate key used in the encryption scheme is based on information that particularly and uniquely identifies the client computer. It does not mean that the key literally has to be such information, but that the key is based on that information in some manner – i.e., derived from such information.

For example, using the identifier of the component 106 that uniquely and particularly identifies computer one as a starting point, embodiments of the invention can convert or otherwise manipulate this information to produce the actual key as may be required by the encryption scheme being used. Each character of the identifier, for instance, may be converted into an eight-bit binary number, the conversions of all such characters concatenated together, and every second or third bit selected until the needed number of bits to make the actual key has been obtained. This is only one example, however, and the invention is not so limited. Thus, when it is stated that information that particularly and uniquely identifies a client computer is used as a key, those of ordinary skill within the art can appreciate that this is shorthand for stating that such information is used as a starting point from which the actual key used by an encryption scheme is derived.

The usefulness of such a key is described in relation to the successful decryption 102 situation, also performed on computer one, and to the unsuccessful decryption 104

situation, performed on a different computer, computer two. In the successful decryption 104 situation, the same component 106 is used to regenerate the first key 114 that was generated as the first key 108 in the encryption 100. Because the same component 106 is being used, the first key 114 regenerated in the successful decryption 102 situation is identical to the first key 108 that was initially generated during the encryption 100 situation. Thus, when the encrypted second key is retrieved from the storage 112, it will be successfully decrypted in 116.

However, in the unsuccessful decryption 104 situation, it is presumed that the encrypted second key was copied from the storage of computer one to a storage of computer two – the storage 122 of FIG. 1. Thus, the component 118 used to regenerate the first key 120 will not be the identical to the component 106 used to generate the first key 108 during encryption. It may have a different serial number, address, or other identifier that is used to particularly and uniquely identifier its computer, which in this case is computer two. Therefore, when the encrypted second key is retrieved from the storage 122, and the regenerated first key is used to decrypt the second key in 124, the decryption will be unsuccessful – because the first key 120 used for decryption necessarily varies from the first key 108 used for encryption, since the first keys are particular and unique to their respective client computers, computer one and computer two, respectively.

Therefore, using a first key to encrypt at least a second key, where the first key is unique and particular to the client computer, controls the distributed use of the second key. The second key as encrypted with the first key may be freely copied to other computers and similar such devices, but it will not be successfully decrypted unless it is decrypted on the computer or similar such device on which it was originally encrypted. In the case of information encrypted with the second key that was purchased by the user of the client computer, this ensures that the user will not be able to copy and use the information on other computers or similar such devices that he or she owns or uses, without the permission and knowledge of the seller of the information. The user may copy the information to other computers freely, but because the first key is unique and particular to the computer on which the second key was encrypted, these other computers will not able to decrypt the second key with their own first keys.

Methods

In this section of the detailed description, methods according to varying embodiments of the invention are described. It is noted that these methods can be computer-implemented. Furthermore, the methods can be realized at least in part as one or more programs, or parts thereof, each having a number of instructions, running on a computer or other such device -- that is, as a program executed from a machine- or a computer-readable medium such as a memory by a processor of a computer or other such device. The programs are desirably storable on a machine-readable medium such as a compact flash memory, floppy disk or a CD-ROM, for distribution and installation and execution on another computer.

Referring to FIG. 2, a flowchart of one method according to an embodiment of the invention is shown. In 200, a first key that is unique and particular to a client is determined, without user intervention. The first key is unique and particular to the client in that it particularly and uniquely identifies the client as compared to other clients. The client is any type of computer or other such device, as is described in a proceeding section of the detailed description. The first key may be one or more of: a processor identifier, a network card address, and a user name in a registry file, as described in the preceding section of the detailed description. The key may also be one or more of: serial numbers and/or the number of cylinders of attached hard disk drives, checksums of the read-only memory (ROM) or other system component's, the Internet Protocol (IP) address of the computer or system, and a combination of installed cards, such as sound, video, SCSI, and other cards, as the key. The first key is not limited to any of these, however. The first key is determined without user intervention in that the first key is not based on input made by the user – that is, the first key is determined with respect to information already contained within the client, such as based on a component thereof, as described in a preceding section of the detailed description (although the invention itself is not so limited).

In 202, at least a second key is encrypted with the first key. The second key may be used to encrypt information such as multimedia information, as described in the preceding section of the detailed description. In 204, the encrypted second key is stored on a storage, such as a non-volatile memory, or a hard disk drive, etc. The invention is not particularly limited to a given type of storage.

In one embodiment of the invention, more information than just the second key is encrypted using the first key. For example, user identification, server addresses, playback

information, program configuration, etc., may be configured, in addition to the second key.

In 206, the encrypted second key is retrieved from the storage, and in 208, the first key is redetermined. If the redetermination of the first key in 208 is performed on the same client as the determination of the first key in 200 was performed, then the redetermined first key in 208 will be identical to the originally determined first key in 200 (assuming that the component used to generate the first key in 200 has not changed or been modified). However, if the encrypted second key was stored on a different client, such that the redetermination in 208 is performed on a different client, then the first key redetermined in 208 will be different than the first key originally determined in 200. In 210, the second key is attempted to be decrypted based on the first key redetermined in 208.

In 212, if the second key was decrypted successfully – that is, if the first key redetermined in 208 was the same as the first key originally determined in 200 -- then the method proceeds to 214, and the method is done. However, if the second key was not decrypted successfully – that is, if the first key redetermined in 208 was not identical to the first key originally determined in 200 – then the method proceeds instead to 216, and the user is notified that the decryption was unsuccessful. In 218, in one embodiment of the invention, the user is requested to reregister the first key with a registering authority. For example, the user may be asked to reregister a purchase of the information that was encrypted with the second key with the seller of the information, by logging onto the seller's web site. The method then proceeds to 214, where it is finished.

It is noted that the invention itself is not limited to the particular embodiment just recited. For example, in some cases, the user may not be notified of unsuccessful decryption. For example, new information may be requested without explaining that any error has occurred, or a web server may automatically be logged onto. Furthermore, in the case of failed decryption, playback or other access to the information may be completely disabled, or allowed only in a limited capacity, without any error notification.

Representative Computer or Other Such Device

In this section of the detailed description, a representative computer or other such device in conjunction with which embodiments of the invention may be practiced, and one or more of which can act as a client or a server as referred to in the previous sections of

the detailed description, is described. However, the invention is not limited to the representative computer or other such device described herein. The phrase "other such device" is used to reflect the fact that devices other than computers can be used in accordance with embodiments of the invention – for example, PDA devices and MP3 devices, although the invention is not limited to an other such device particularly recited herein.

The computer or other such device is shown in block diagram form in FIG. 3. The computer or other such device 400 desirably includes one or more of desirably but not necessarily each of the following components. The display 402 can include a flat-panel display, such as a liquid crystal display (LCD), or a cathode-ray tube (CRT) display. The input device 404 can include a keyboard, a pointing device such as a mouse, trackball or touch pad, a touch screen, one or more buttons, etc. The processor 406 executes instructions implementing methods of varying embodiments of the invention. In one embodiment, the processor 406 can be considered the means to perform a method according to an embodiment of the invention. The communications device 408 can be used to communicate with another computer or other such device – to communicate with a client, for example, in the case of a server, and vice-versa. The device 408 may be a network adapter, a modem, a wireless transceiver, etc. The non-volatile storage 410 can include a hard disk drive, and/or non-volatile memory such as flash and compact flash memory, such as in the form of memory cards. The volatile memory 412 typically includes a version of dynamic random-access memory (DRAM), as known within the art.

Other Embodiments to Promote Fraud Prevention and Security

In this section of the detailed description, additional embodiments of the invention are described designed for promoting security and fraud prevention. Three particular additional embodiments are described: a checksum embodiment in conjunction with FIG. 4, a piracy signature detection embodiment in conjunction with FIG. 5, and a recording inputs variance embodiment in conjunction with FIG. 6. Each of these is now described in turn.

Referring first to FIG. 4, a flowchart of a method of a checksum embodiment of the invention is shown. In 300, a checksum is determined for a player of information, the information itself, or both. The player can be a viewer for text information, or a player for multimedia information such as audio, music, video and image information. That is, the

player can be playback software for the information. The information itself can be any type of information, such as text information or multimedia information. Still other information amenable to embodiments of the invention includes software programs, such as the electronic distribution thereof. The checksum is a value known within the art, and is a value used to ensure that data is stored or transmitted without modification. It is created in one embodiment by calculating the binary values in the data using an algorithm (the specific type of which the invention is not particularly limited to), and storing the results with the data, where the data in this case is the player of the information, the information itself, or both. Thus, the player and/or the information already have a predetermined checksum target value associated therewith.

In 302, it is determined whether the checksum determined in 300 matches the checksum target value. A non-match indicates that the player, the information, or both, have been modified. Because such modification may indicate that the player, the information, or both have been changed for piracy or other fraudulent purposes, the information will not be played back or otherwise allowed to be accessed if such a non-match occurs. In this situation, the method proceeds from 304 to 306, and a checksum error is indicated. Otherwise, the method proceeds from 302 to 304, where the method is finished.

In one particular embodiment, a checksum is stored in a data block that also contains the second key, as the second key has been described in preceding sections of the detailed description. The checksum is determined from the unencrypted version of the data block in this embodiment, before it is encrypted with the first key and stored. Thus, this provides for easy determination as to whether the block has been decrypted successfully. If the checksum matches the newly calculated checksum, then the block has been reconstructed successfully. Furthermore, if the data block has been modified while encrypted, this is also able to be detected, because the checksums will not match.

Referring next to FIG. 5, a flowchart of a method of a piracy signature detection embodiment of the invention is shown. In 500, one or more system indicators are each checked against a signature database of known piracy mechanism. Each of the system indicators in one embodiment is an operating system file, such as those typically saved in the windows subdirectory of the root hard drive in computers running versions of the Microsoft Windows operating system. However, the invention is not so limited. Other system indicators include the boot sectors of the root hard drive, as known within the art,

as well as various places within the memory of the client. The signature database contains information regarding the binary patterns of the machine code of a particular known piracy mechanism, such as a computer program or a virus (although the invention is not particularly limited to either as a piracy mechanism) meant to encourage piracy of software and/or other information, such as text and multimedia information. Thus, the database of piracy patterns is compared with existing files and other system indicators to determine if a piracy mechanism is present. If such a piracy mechanism is present in any of the system indicators, then playback of the information is prevented in 502. Furthermore, in 504, the signature database can be periodically updated so that it remains current, and is able to detect new piracy mechanisms, for example, by downloading a new database or an update file from a web site.

In one particular embodiment, detection of a modification or piracy mechanism is reported to the user. However, the invention is not so limited. In other embodiments of the invention, detection may result in the disabling of playback or other access to the underlying information; notification of a server that piracy or other modification mechanisms have been found; and/or, modification of the player, the information, or other files that are present on the system to prevent them from being used at all, or to cause them to function only in a limited capacity (e.g., playing music at a reduced quality level, or playing only 20% of a song). In another embodiment, at least one of these actions also occurs if the first key does not successfully decrypt the second key, as described in preceding sections of the detailed description.

The invention is not particularly limited to the manner by which the signatures of the piracy or other modification mechanisms are determined. In one embodiment, however, a signature includes a checksum of the offending piracy or other modification mechanism. This provides for easy detection of the mechanism.

Referring finally to FIG. 6, a diagram of a recording inputs variance embodiment of the invention is shown. The player 600 is in one embodiment playback software for playing back information of a predetermined type, such as multimedia information like audio and video information. When the player 600 plays back the information, the information is sent over outputs, such as audio or video outputs, via the operating system, so that it can be heard on a speaker 602, in the case of audio information, for example, or another output actuation device, such as a display in the case of video information. In some operating systems, such as versions of the Microsoft Windows operating system, the

information is also output such that it can be received by recording inputs, so that it can also be recorded by a recording device, as represented by the microphone 604 in FIG. 6 (although the invention is not limited to such a recording device).

Therefore, to prevent unauthorized recording of information that is being played back for output on an output actuation device, the levels of the recording inputs, such as the volume level of the recording inputs or other levels, are varied during playback, as represented by 606 in FIG. 6. This results in an unsatisfactory recording. While the information may still be present on the recording, the volume level may be constantly changing, for example, such that the recording is essentially useless. As another example, in the case of video multimedia information, the color levels may be constantly changing, such that the picture is still recognizable, but of unsatisfactory condition. The means for varying the recording inputs in one embodiment of the invention can be considered a computer program, which may also by the computer program that is responsible for playing back the information itself (for example, the player 600).

In other embodiments of the invention, other outputs and/or inputs are varied instead of or in addition to the recording inputs, in order to prevent unauthorized recording of information that is being played back for output on an output actuation device. Furthermore, in one embodiment of the invention, such outputs and/or inputs, such as the recording inputs, are muted. The term varying the volume level is inclusive of muting, however.

Conclusion

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

I claim:

1. A computer-implemented method for a client characterized by:
determining (200) a first key unique and particular to the client without user intervention;
encrypting (202) at least a second key with the first key; and,
storing (204) the second key as encrypted with the first key on a storage.

2. The method of claim 1, further characterized by:
retrieving (206) the second key as encrypted with the first key from the storage;
redetermining (208) the first key; and,
decrypting (210) the second key with the first key as redetermined.

3. The method of claim 2, further characterized by:
determining (212) whether decrypting the second key was successful; and,
upon determining that decrypting the second key was unsuccessful, indicating (216) so to the user.

4. The method of claim 3, further characterized by, upon determining that decrypting the second key was unsuccessful, requesting (218) that the user reregister the first key with a registering authority.

5. The method of claim 1, wherein the first key is at least one of: a processor identifier, a network card address, an IP address, a checksum of a component, a serial number of a hard disk drive, a number of cylinders of a hard disk drive, and a user name in a registry file.

6. The method of claim 1, wherein the method is performed by execution of a computer program by a processor from a computer-readable medium.

7. A computer-implemented method characterized by:
determining (300) a checksum for at least one of: a player, and information;

comparing (302) the checksum against a target value; and,

indicating (304) a checksum error upon determining that the checksum does not match the target value.

8. The method of claim 7, wherein the information is one of: text information, and multimedia information.

9. The method of claim 7, wherein the method is performed by execution of a computer program by a processor from a computer-readable medium.

10. A computer-implemented method characterized by:

for each of at least one system indicators, checking (500) the system indicator against a signature database of known piracy mechanisms; and,

upon determining a known piracy mechanism in any of the at least one system indicators, preventing (502) playback of information.

11. The method of claim 10, further characterized by periodically updating (504) the signature database.

12. The method of claim 10, wherein the information is one of: text information, and multimedia information.

13. The method of claim 10, wherein the method is performed by execution of a computer program by a processor from a computer-readable medium.

14. A computer-implemented method characterized by:

playing back multimedia information of a predetermined type; and,

while playing back the multimedia information of the predetermined type, varying at least one of inputs and outputs for the predetermined type to prevent unauthorized copying of the multimedia information.

15. The method of claim 14, wherein the predetermined type is at least one of: audio information, and video information.

16. The method of claim 14, wherein the method is performed by execution of a computer program by a processor from a computer-readable medium.

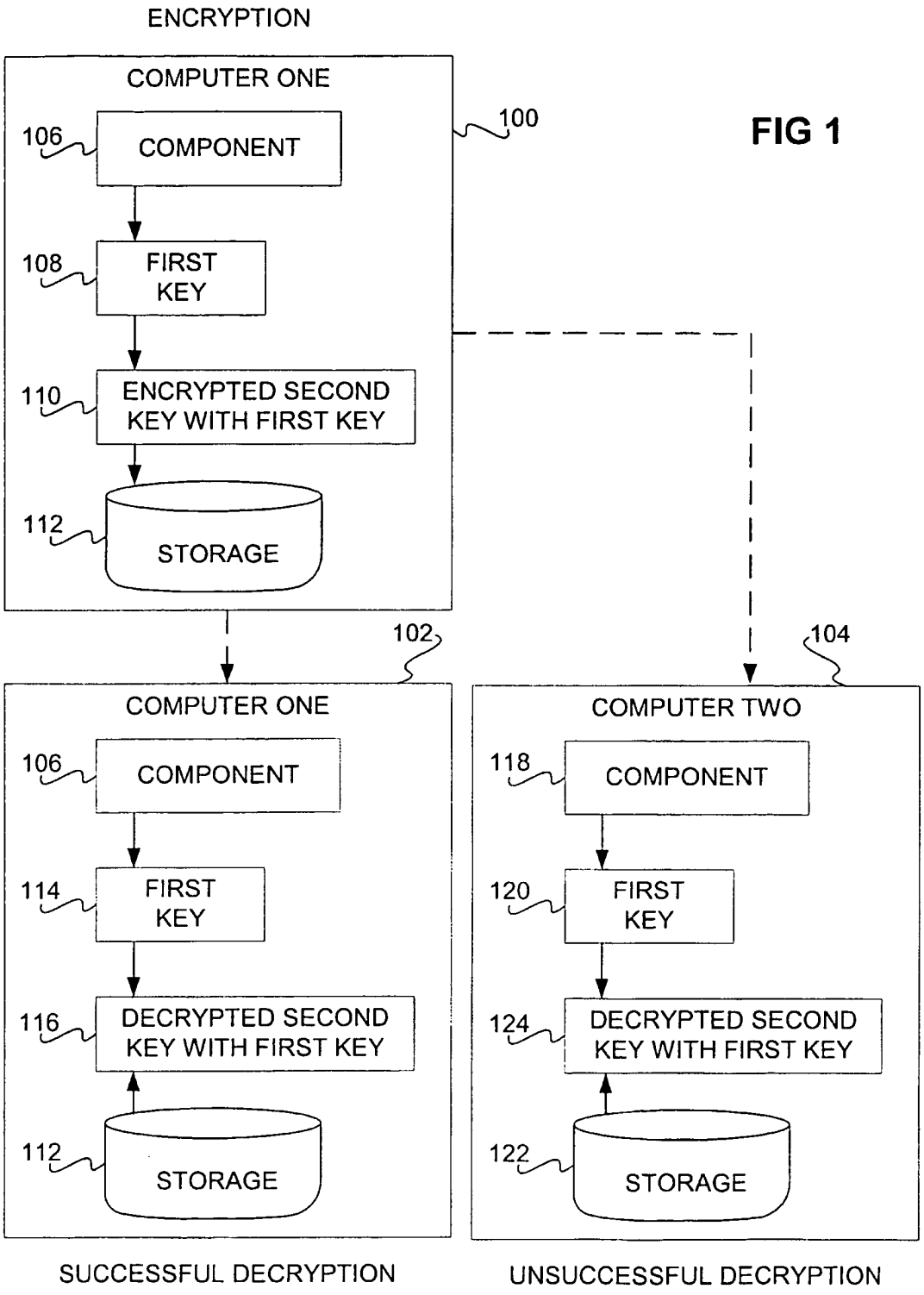

ENCRYPTION
COMPUTER ONE
100
106
COMPONENT
108
FIRST KEY
110
ENCRYPTED SECOND KEY WITH FIRST KEY
112
STORAGE
102
104
COMPUTER ONE
106
COMPONENT
114
FIRST KEY
116
DECRYPTED SECOND KEY WITH FIRST KEY
112
STORAGE
COMPUTER TWO
118
COMPONENT
120
FIRST KEY
124
DECRYPTED SECOND KEY WITH FIRST KEY
122
STORAGE
SUCCESSFUL DECRYPTION
UNSUCCESSFUL DECRYPTION

FIG 1

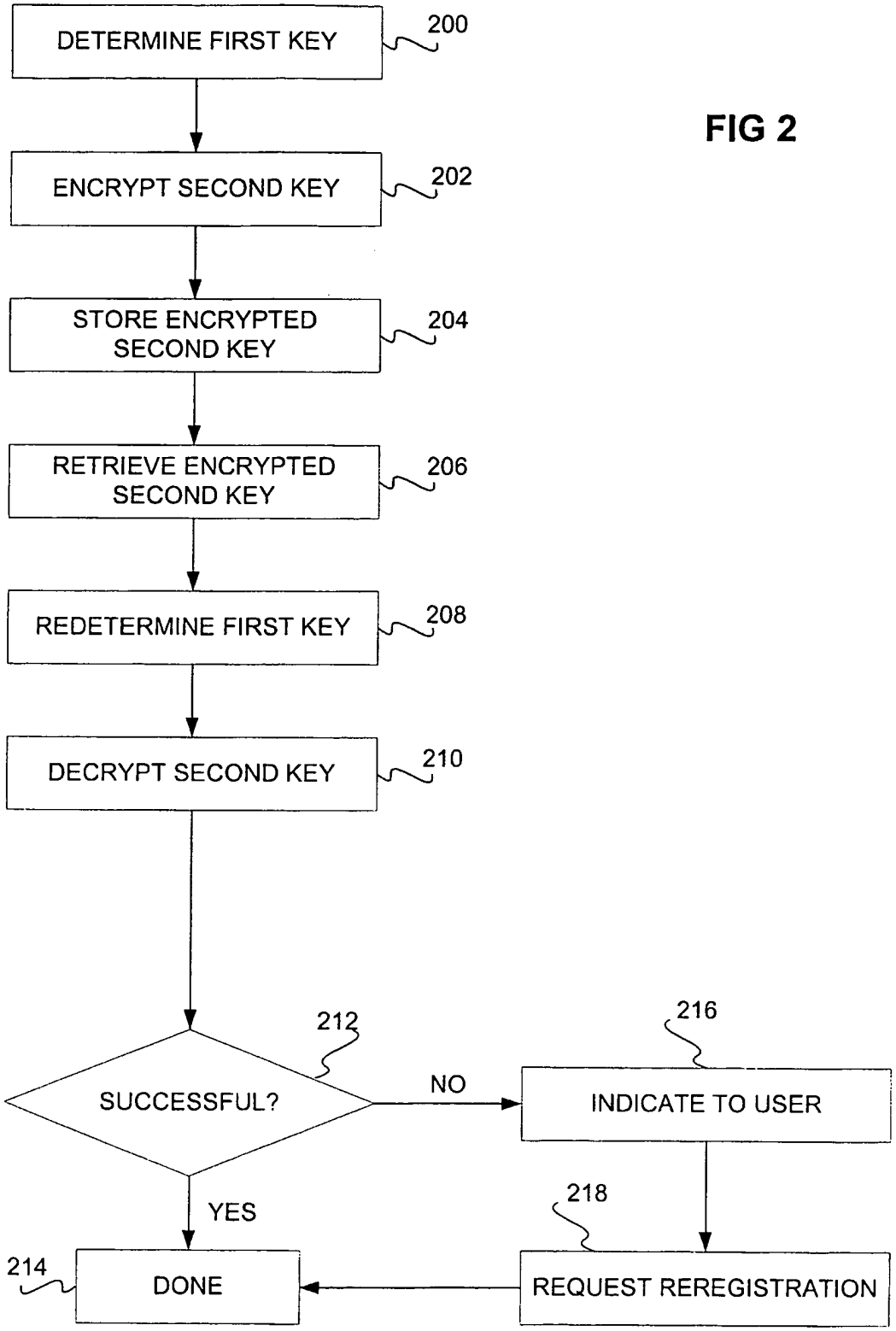

DETERMINE FIRST KEY
200
ENCRYPT SECOND KEY
202
STORE ENCRYPTED SECOND KEY
204
RETRIEVE ENCRYPTED SECOND KEY
206
REDETERMINE FIRST KEY
208
DECRYPT SECOND KEY
210
212
SUCCESSFUL?
NO
216
INDICATE TO USER
YES
218
214
DONE
REQUEST REREGISTRATION

FIG 2

FIG 3

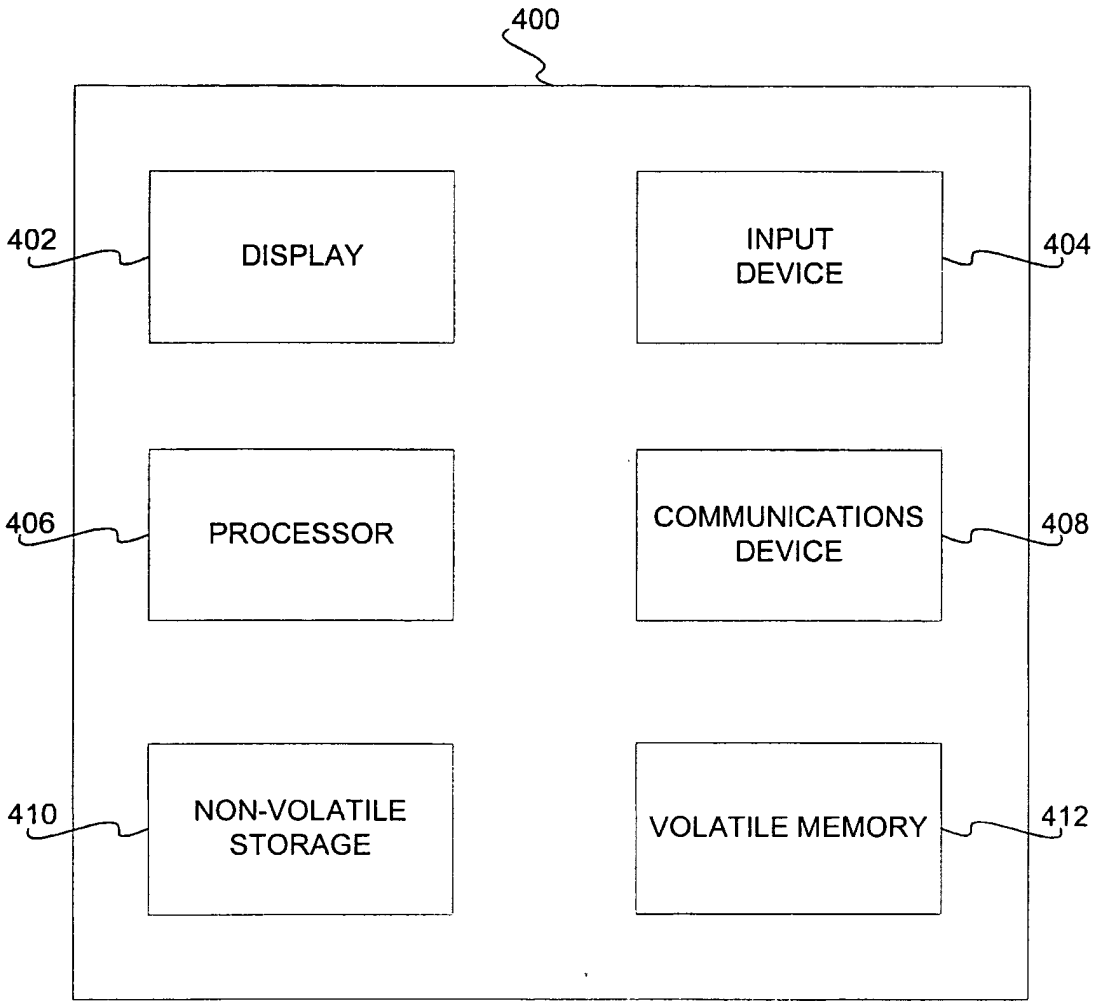

400
402
DISPLAY
INPUT DEVICE
404
406
PROCESSOR
COMMUNICATIONS DEVICE
408
410
NON-VOLATILE STORAGE
VOLATILE MEMORY
412

FIG 4

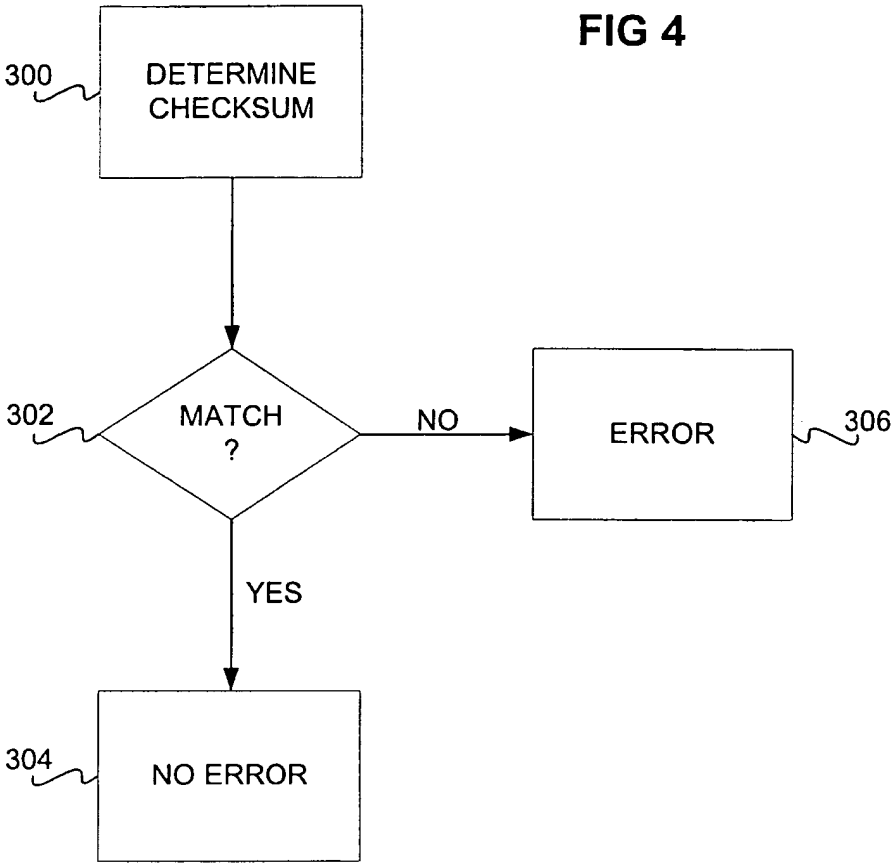

300
DETERMINE CHECKSUM
302
MATCH ?
NO
ERROR
306
YES
304
NO ERROR

FIG 5

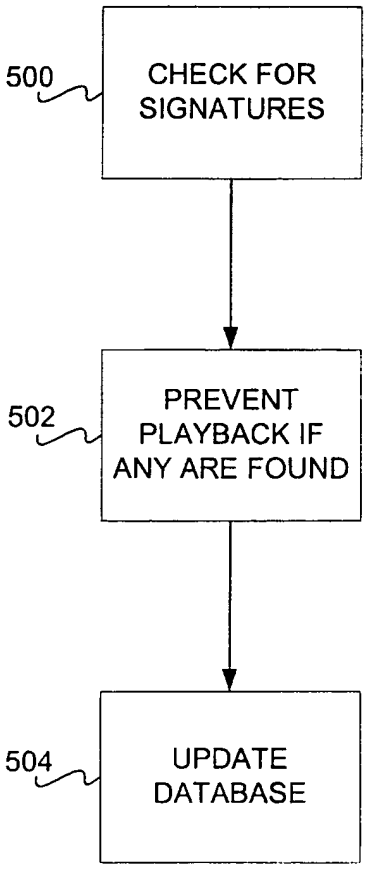
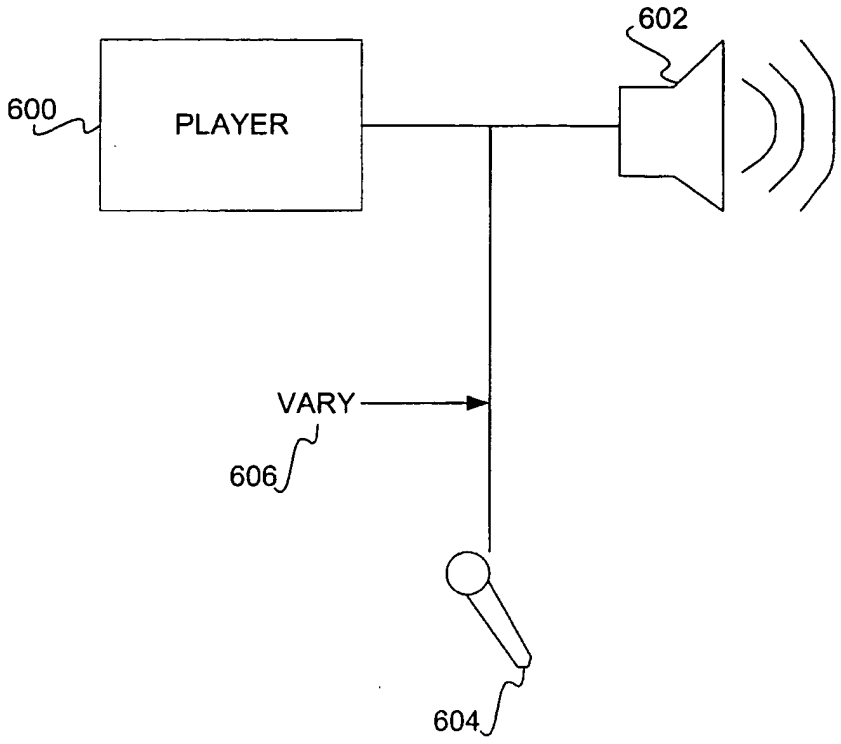

500
CHECK FOR SIGNATURES
502
PREVENT PLAYBACK IF ANY ARE FOUND
504
UPDATE DATABASE

FIG 6



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31839 A3

(51) International Patent Classification[7]: H04L 9/08, G06F 1/00

(21) International Application Number: PCT/US00/29184

(22) International Filing Date: 21 October 2000 (21.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/425,861 23 October 1999 (23.10.1999) US

(71) Applicant: LOCKSTREAM CORP. [US/US]; 13033 Bellevue-Redmond Road, Bellevue, WA 98005 (US).

(72) Inventor: SEARLE, Scott; 218 Main Street, Suite 441, Kirkland, WA 98033 (US).

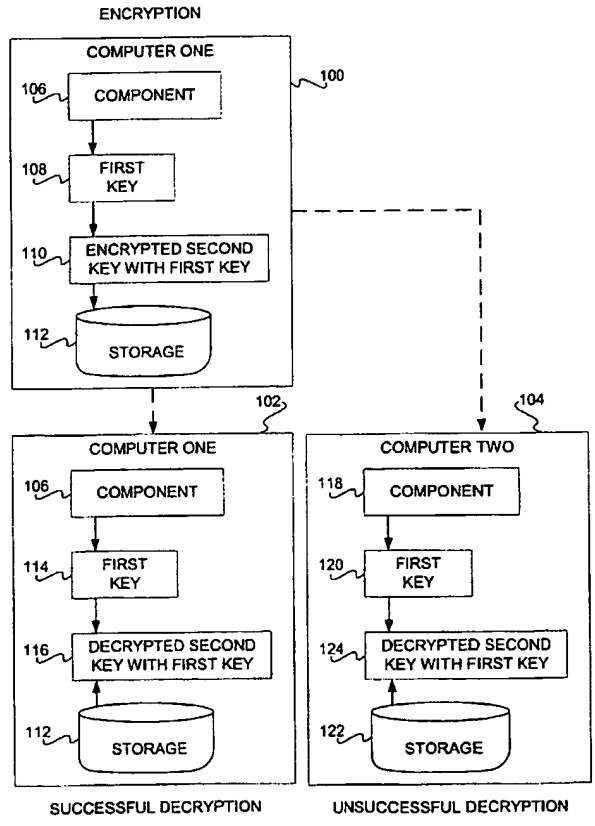
(74) Agents: LERNER, Lawrence, I. et al.; Lerner, David, Littenberg,, Krumholz & Mentlik, LLP, 600 South Avenue West, Westfield, NJ 07090 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: KEY ENCRYPTION USING CLIENT-UNIQUE ADDITIONAL KEY



(57) Abstract: Encryption of a key using another key that is unique and particular to a given client is disclose. In one embodiment, a computer-implemented method determines a first key that is unique and particular to the client, without user intervention. In varying embodiments, this key can be one or more of: a processor identifier, a network card address, an IP address, a checksum of a component, a serial number of a hard disk drive, a number of cylinders of a hard disk drive, and a user name in a registry file. At least a second key that provides access to information, such as multimedia information, is encrypted with this first key. The second key as encrypted with the first key may be stored on a storage.

WO 01/31839 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
22 November 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/US 00/29184

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 933 497 A (CORRIGAN MICHAEL JOSEPH ET AL) 3 August 1999 (1999-08-03) column 4, paragraph 1 column 5, line 44 - line 50 column 7, line 23 - line 26 column 9, line 21 - last line	1,2,5,6
X	US 5 337 357 A (CHOU WAYNE W ET AL) 9 August 1994 (1994-08-09) column 1, line 45 -column 2, line 3 column 2, line 57 -column 4, line 37 abstract	1,2,5,6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 March 2001	14. 06. 2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	HOLPER, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ernational application No.
PCT/US 00/29184

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-6

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-6

   A method for a client comprising the steps of determining a first key unique to the client and of encrypting and storing at least a second key with the first key.

2. Claims: 7-9

   A method for determining a checksum for at least one of a player and an information, comparing the checksum against a target value and indicating a checksum error.

3. Claims: 10-13

   A method for checking a system indicator against a signature database of known piracy mechanisms and for preventing playback.

4. Claims: 14-16

   A method for varying, during playback of multimedia information, at least one of inputs and outputs to prevent unautorized copying of the multimedia information.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. tional Application No
PCT/US 00/29184

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5933497 A	03-08-1999	JP 2066371 C	24-06-1996
		JP 5334072 A	17-12-1993
		JP 7099497 B	25-10-1995
US 5337357 A	09-08-1994	CA 2120816 A	18-12-1994
		EP 0636962 A	01-02-1995